WHAT IS CLAIMED IS:

1. A method comprising:

receiving, at a BIOS, a message from an authorized party;

authenticating the message; and

controlling a state of a feature of a system resource, using the BIOS, according to the message.

2. The method of claim 1 further comprising verifying an identifier in the message against a unique system identifier of the system.

3. The method of claim 1 further comprising writing the message into a secure non-volatile location.

4. The method of claim 3 wherein the secure non-volatile location comprises a remote storage.

5. The method of claim 1 further comprising splicing the content of the message into an execution path of the BIOS.

6. The method of claim 1 further comprising loading and executing content of the message using the BIOS at run-time.

16. The method of claim 1 further comprising updating a feature set of the BIOS according to the message.

6. A system comprising:

a system resource having controllable features;

a non-volatile memory that stores a BIOS, the BIOS being adapted to receive a secure message from an authorized party for controlling at least one of the features.

7. The system of claim 6 further comprising a write-once non-volatile unit for storing a public key accessible by the BIOS.

8. The system of claim 6 wherein the BIOS includes authentication circuitry for authenticating the secure message with a public key.

9. The system of claim 6 further comprising a write-once non-volatile unit for storing a unique system identifier accessible by the BIOS.

10. The system of claim 6 wherein the BIOS also includes verification circuitry for verifying an identifier in the message against a unique system identifier.

11. The system of claim 6 further comprising a secure non-volatile location for storing the at least one of the optional features to be enabled, the location being readable and writable by the BIOS.

12. The system of claim 11 wherein the location comprises a remote storage.

13. The system of claim 6 wherein the BIOS also includes a feature set that is updated according to content of the secure non-volatile storage.

14. The system of claim 6 wherein the BIOS also includes a feature set that is updated according to content of the secure non-volatile storage.

15. The system of claim 6 wherein the BIOS loads and executes the content of the message at run-time.

16. A computer program product residing on a computer readable medium comprising instructions for causing a computer to:

receive, at a BIOS, a message from an authorized party;

authenticate the message; and

control a state of a feature of a system resource, using the BIOS, according to the message.

17. The computer program product of claim 16 further comprising instructions for causing a computer to verify an identifier in the message against a unique system identifier of the system.

18. The computer program product of claim 16 further comprising instructions for causing a computer to write the message into a secure non-volatile location.

19. The computer program product of claim 18 wherein the secure non-volatile location comprises a remote storage.

20. The computer program product of claim 16 further comprising instructions for causing a computer to splice the content of the message into an execution path of the BIOS.

23
21. The computer program product of claim 16 further comprising instructions for causing a computer to load and execute the content of the message at the BIOS at run-time.

24
22. The computer program product of claim 16 further comprising instructions for causing a computer to update a feature set of the BIOS according to the message.